Datasheet

ThreatVision

TEAMT5

Drive Decisions and Strengthen Resilience with Expert Intelligence

ThreatVision Threat Intelligence Platform

Built on 20+ years of APAC threat research, ThreatVision provides high-quality, focused intelligence on malware and APT groups. It integrates strategic, operational, and tactical intelligence to help decision-makers, risk managers, and IR teams understand the threat landscape and strengthen defenses.
ThreatVision also provides deep and dark web intelligence to detect early warnings and data breach risks. With coverage of forums, marketplaces, and social media, its automated alerts and custom reports allow organizations to proactively address threats before they escalate.

Key Numbers

1,800+	6.7 M+	26 M+	3,100+	300+
Reports	IoCs	Samples	Malware	Adversaries

ThreatVision Core Values

Rapid Threat Identification

Integrates multiple IoC sources to quickly identify hidden attacks and enhance defensive efficiency.

Precise Threat Analysis

Offers sample submission and analysis to rapidly identify malicious characteristics for IR and investigations.

Full Attack Context

Correlates malware with adversaries to reconstruct attack context, motives, and objectives.

APAC Intelligence Expertise

Integrates multiple IoC sources to quickly identify hidden attacks and enhance defensive efficiency.

Real-time Intelligence Access

Instantly query IPs, domains, and samples for raw intelligence, with options for custom reports and tools.

Fast Integration & Automation

Connects with TIP and SIEM platforms to automate intelligence feeds and accelerate incident response.

The Importance of Threat Intelligence

ThreatVision provides three levels of intelligence to support diverse security roles, from executive decision-making to frontline defense.

Strategic Intelligence for Decision-Makers	Operational Intelligence for Security Teams	Tactical Intelligence for Frontline Defenders
Provides CISOs with a high-level view of the threat landscape, linking cyber threats to business impact to inform strategy and resource allocation.	Details adversary TTPs, motives, and campaigns, helping frontline teams prioritize and tailor response efforts.	Delivers actionable, technical data on TTPs for immediate use in detection and defense by IT and security teams.

A Closer Look at ThreatVision Reports

ThreatVision provides four main categories of intelligence reports: APAC APT intelligence, vulnerability intelligence, Chinese cyberworld & China cyber policy, and cybercrime intelligence, helping organizations make informed decisions and gain advantages.

APT in Asia Flash Reports
(aka Flash Report)

Focuses on the latest APT attack incidents, analyzing techniques and technical details while providing relevant IoCs. Flash Report is published twice a week, with at least 100 reports per year.

APT in Asia Monthly Reports
(aka Monthly Report)

Summarizes the past month's APT dynamics in the APAC region, linking geopolitical situations with attack behaviors. Each report covers an average of 13 to 16 incidents and provides relevant IoCs. Monthly Report is published once a month, totaling 12 per year.

APT Campaign Tracking Reports
(aka CTR)

Provides in-depth analysis of threat groups, attack tactics, and target scopes to enhance a comprehensive understanding of significant adversaries and campaigns in the APAC region. CTR is published twice per quarter, totaling 8 issues per year, including 6 adversary group analysis reports and 2 semiannual threat landscape review reports.

Cyber Affairs Biweekly Reports
(aka Biweekly Report)

Offers in-depth analysis of the cyber capabilities of emerging power China, as well as cybersecurity news, policies, regulations, and security incidents in the Chinese-speaking online world. Biweekly Report is published every two weeks, totaling 24 per year.

Vulnerability Insights Reports
(aka VIR)

Focuses on one critical vulnerability at a time, providing detailed technical intelligence, potential attack scenarios, and detection tools. VIR is published every two weeks, totaling 24 per year.

Patch Management Reports
(aka PMR)

Compiles approximately 100 high-risk vulnerabilities, including proof-of-concept (PoC) details, affected products, and patching recommendations to help prioritize remediation efforts. PMR is updated weekly, totaling 52 per year.

Cybercrime Intelligence Reports
(aka CC Report)

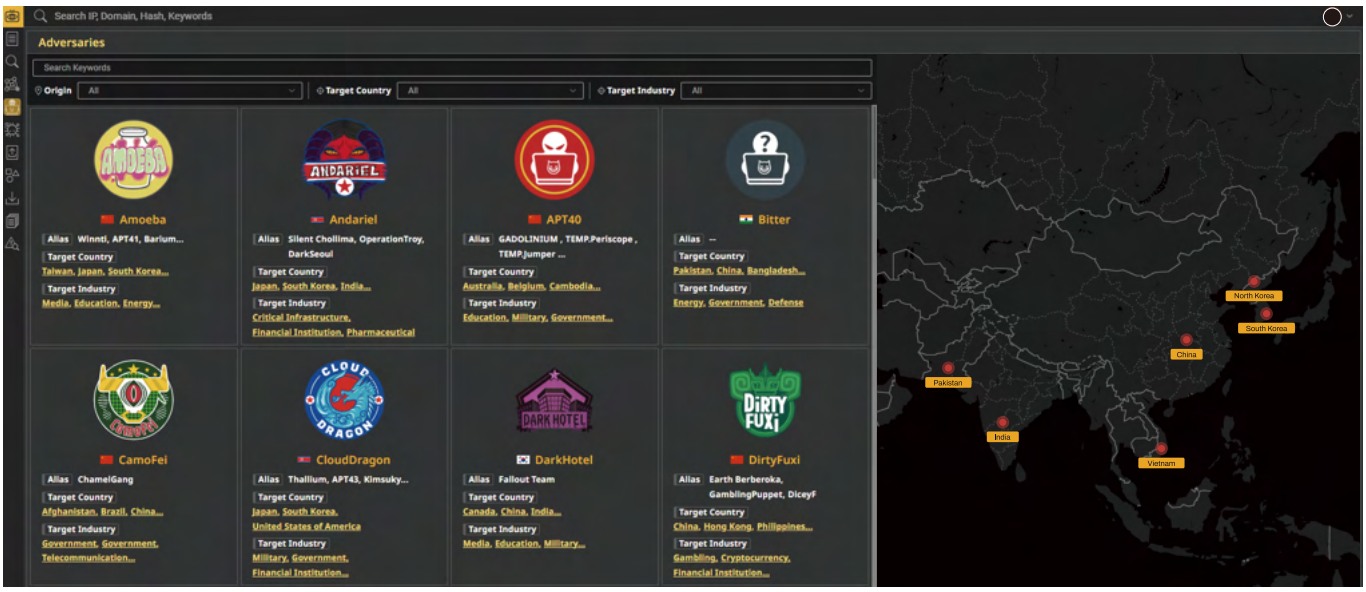
The Cybercrime Intelligence Reports (CC Reports) are built on TeamT5's long-term research and monitoring of the deep web, dark web, and criminal communities. The series includes Cybercrime Campaigns (published monthly, 12 issues per year) and both Forum Activities and Ransomware Activities (each published at least four times per month, totaling a minimum of 48 issues per year).

ThreatVision Key Highlights

APT/Cyber Crime IoCs	Threat Hunting Tools	Request for Information (RFI)	API Ready
APT IoCs focus on state-sponsored attacks; Cyber Crime IoCs strengthen defenses against large-scale cyber crime activities. Both are released once weekly, total 52 per year each.	Provide analyst-designed rules to scan environments, uncover threats and accelerate investigation.	Offer tailored research on specific topics or attack campaigns to facilitate risk assessments and defenses.	Enable automated intelligence integration into existing platforms, ensuring faster deployment and consistent operation.

ThreatVision Platform Overview

ThreatVision's diverse intelligence supports various roles and tasks, helping organizations fully grasp the behavioral patterns of adversaries and proactively deploy defensive strategies. It is the optimal solution from strategic planning to frontline defense.



Get Started with ThreatVision

Please contact the TeamT5 sales team to request a 14-day trial account for ThreatVision. For further information, please email sales@teamt5.org. We look forward to helping protect your organization from cyber threats.

About TeamT5

v.202605

Widely trusted by more than 550 customers around the world, including government departments, technology, manufacturing, finance, medical care, military, telecommunications and other industries.

TeamT5 has more than 20 years of experiences in malware and advanced persistent penetration attacks (APT). With language and cultural advantages, we possess specific expertise in cyber espionage in the Asia-Pacific region, and are often invited to present the latest information at world-class cybersecurity conferences, including Black Hat in the United States, Code Blue / AVTokyo in Japan, Troopers in Germany, and Hack In The Box and FIRST. As a world-leading team in the field of threat intelligence research and advanced cybersecurity technology, we have also been interviewed by Bloomberg and CNN in the United States, Sankei Shimbun and Asahi Shimbun in Japan, and ET News in South Korea.

Tel +886-2-7706-1299
E-mail sales@teamt5.org

TEAMT5 | THREAT INTELLIGENCE PIONEER, BORN IN ASIA